



43 Milliarden Euro Schaden durch Attacken auf deutsche Industrie

Ein Gesamtschaden von insgesamt 43,4 Milliarden Euro ist der deutschen Industrie in den vergangenen beiden Jahren durch Sabotage, Datendiebstahl oder Spionage entstanden. Das ist das Ergebnis einer Studie des Digitalverbands Bitkom.

Achim Berg, Bitkom-Präsident, dazu:



IT- oder Telekommunikationsgeräte wurden in den vergangenen zwei Jahren bei einem Drittel der Unternehmen gestohlen, bei fast einem Viertel sind sensible digitale Daten abgeflossen.

Digitale Sabotage

19 Prozent der Industrieunternehmen berichten von digitaler Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen. Weitere 28 Prozent vermuten, dass es solch einen Vorfall bei ihnen gab. Bei 11 Prozent wurde die digitale Kommunikation ausgespäht, beispielweise E-Mails oder Messenger-Dienste.

Thomas Haldenwang, Vizepräsident des [Bundesamtes für Verfassungsschutz](#) (BfV), betont:



Bei fast der Hälfte der Befragten (47 Prozent) haben digitale IT-Angriffe einen Schaden verursacht.

Analoge Attacken vergleichsweise gering

Klassische analoge Attacken sind für die Industrie auch ein Thema, fallen aber vergleichsweise weniger ins Gewicht: 21 Prozent der Befragten haben einen Diebstahl von sensiblen physischen Dokumenten, Unterlagen, Mustern oder Maschinen festgestellt. Bei 10 Prozent kam es in den vergangenen zwei Jahren zur analogen Sabotage von Informations- und Produktionssystemen oder Betriebsabläufen, zum Beispiel durch die Manipulation von Geräten vor Ort in Unternehmen.

Thomas Haldenwang erklärt:



Kritische Unternehmensdaten im Visier

Angreifer haben im Rahmen ihrer Attacken unterschiedlich sensible Daten erbeutet. Bei fast der Hälfte (48 Prozent) der betroffenen Industrieunternehmen wurden

Kommunikationsdaten wie E-Mails gestohlen. Bei jedem fünften Unternehmen sind durch digitale Angriffe jeweils Kundendaten und Finanzdaten abgeflossen.

Patente und Ergebnisse aus Forschung und Entwicklung sind bei jedem zehnten Unternehmen in kriminelle Hände gefallen.

Achim Berg meint:



Täter aus eigenen Reihen

Bei 63 Prozent der Betroffenen gingen Delikte von ehemaligen oder derzeitigen Mitarbeitern aus. Die Hälfte der geschädigten Unternehmen (48 Prozent) hat Kunden, Lieferanten, externe Dienstleister oder Wettbewerber als Täter identifiziert.

Bei 29 Prozent waren es Privatpersonen oder Hobbyhacker, 17 Prozent der Betroffenen berichten von organisierter Kriminalität, jedes neunte betroffene Unternehmen gibt ausländische Nachrichtendienste als Täter an.

Mitarbeiter als effektivster Schutz

Aber kriminelle Handlungen werden auch häufig durch aufmerksame Mitarbeiter aufgedeckt. Sechs von zehn betroffenen Industrieunternehmen (61 Prozent) sind so erstmalig auf Angriffe aufmerksam geworden. 40 Prozent der Betroffenen erhielten Hinweise auf Angriffe durch eigene Sicherheitssysteme, bei fast einem Viertel war es hingegen reiner Zufall. Nur bei 3 Prozent der Unternehmen gingen erste Hinweise auf Delikte durch externe Strafverfolgungs- oder Aufsichtsbehörden ein.

Künftige Bedrohung: digitale Angriffe

Nahezu alle Befragten (97 Prozent) nennen sogenannte Zero-Day-Exploits als größte Gefahr. Dabei nutzen Angreifer Sicherheitslücken in Software aus, die bis dahin unbekannt waren. 93 Prozent fürchten die Infizierung mit Schadsoftware, 68 Prozent geben den Mangel an qualifizierten IT-Sicherheitskräften als Bedrohung an. Die zunehmende Fluktuation von Mitarbeitern ist für 58 Prozent der Unternehmen ein Risiko.

Dass Kriminelle die Rechenleistungen von Internetnutzern anzapfen, etwa zum unbemerkten Schürfen von Kryptowährungen, nehmen hingegen nur 29 Prozent der Unternehmen als echte Gefahr wahr.

Bild: © alphaspirt / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4945415/43-milliarden-euro-schaden-durch-attacken-auf-deutsche-industrie/>